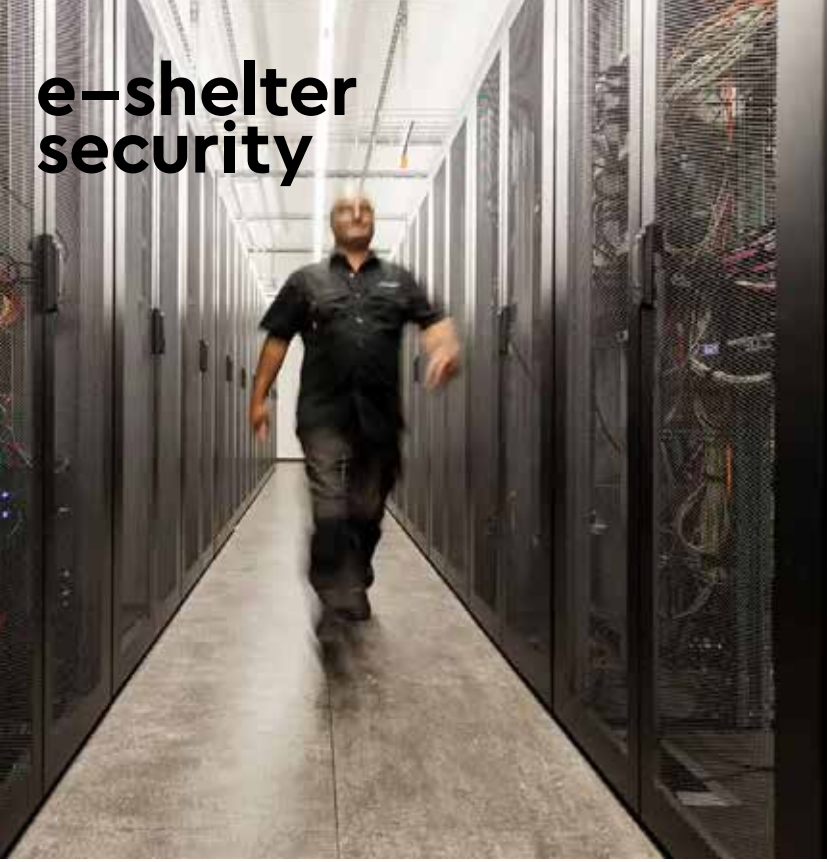
e–shelter
security



— Physical Protection of Critical Infrastructures

Intelligently networked. User-centered. Automated.

— Contents

3
Challenge

5
Solution

12
Effective Perimeter Protection

15
Automated Access Process

21
Monitoring and Hazard Management

24
Strong Partners

27
Your Advantages

29
Our Experience

— Challenge

Whether it is a data centers, energy supply, life science or production and logistics – operators of critical infrastructures face special challenges. Due to the volatile geopolitical situation and changing regulatory framework, the physical protection of companies and facilities is becoming increasingly important.

In order to meet the new requirements of the KRITIS umbrella law and the underlying EU Directive on the Resilience of Critical Facilities (CER) operators must meet minimum standards in the areas of access control and perimeter protection and central monitoring of security-relevant events.

Learn how to sustainably protect people and assets through holistic security solutions while enabling efficient operations by means of intelligent process automation.

Problems that we solve:

Inadequate detection of threats due to a lack of intelligent analysis functions and a failure to network security systems.

Lack of central monitoring and management of events as well as KPIs and data for the optimization of systems and processes in business operations.

Personnel-intensive operations due to the absence of digitalization measures, and process automation due to the shortage of skilled workers constitute an increasing operational risk.

— Solution

We enable the reliable detection of hazards and convert sensor data into automated actions for an efficient security management.

— Sense

Multi-level safety systems and IoT sensors

→ Reliable data and early detection of hazards

— Analyze

Decentralized intelligence and unified security platform

→ Focusing on relevant events, central control

— Act

Intelligently networked systems, digitized processes and managed services

→ User experience, efficiency and economy

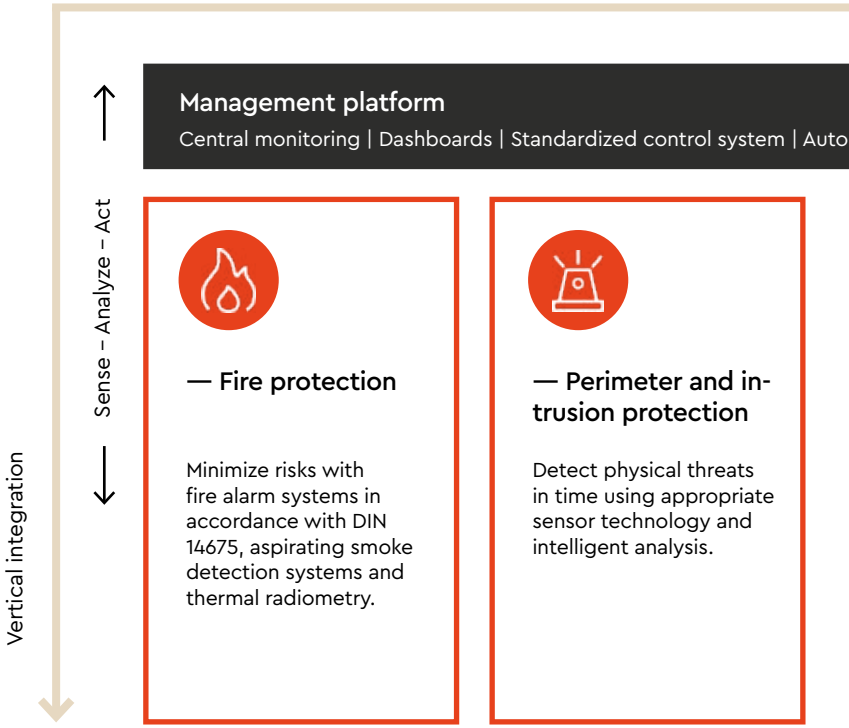
Automation

— Portfolio Overview

With our many years of experience in installation and system integration within critical infrastructure, we implement vendor-independent integrated security solutions with tailored functionality.

These are created on the basis of a security concept that takes into account individual security goals and regulatory requirements.

The modular portfolio includes integrated solution modules from fire protection to building digitization. With the help of a management platform, all security systems are connected in a uniform way and enable central monitoring.



Horizontal integration

mated actions | Case management of alarms in a control center

— Video surveillance and analysis

Monitor processes and protect assets and people with intelligent video technology.

— Access control system

Benefit from automated and secure processes in access management.

— Building IoT

Enable sensor-based analysis of space utilization and ensure usage-based control of building systems and a digital workplace experience.

— Core Components

With our holistic security solutions we support you in the efficient implementation of your technical security concept. Three components are crucial for the physical protection of critical infrastructures:

— Perimeter protection

Intelligent perimeter protection is the most effective measure to prevent physical threats and is designed in such a way that an attack can be fended off according to the risk profile.

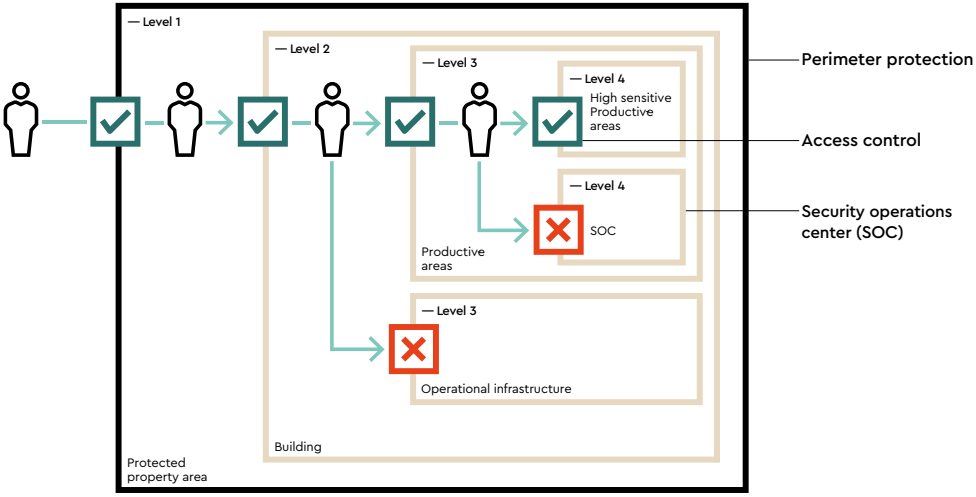
— Access control

The access control system ensures that only authorized and verified persons and vehicles are granted access to the company premises and to defined security zones. Documented authentication takes place at every zone transition – depending on the protection class in conjunction with separation and biometric procedures.

— Monitoring and hazard management

The heart of a holistic security solution is the certified control center (VdS 3138–2). Here, security-relevant events are combined into a uniform overview of the situation and processed quickly and specifically on the basis of defined workflows.

Video technology and analysis are an integral part of access control, perimeter and campus security. A wide range of hazard detection systems are used to trigger alarms in the event of unauthorized access. In accordance with DIN 14675 our fire alarm systems provide basic protection for your site.



— Safety zones and protection categories

Depending on the purpose of the site to be protected, safety zones are formed which combine areas with the same or similar requirements. For those zones, the safety concept defines protection categories (levels 1–4), from which the requirements for the security systems are derived, in particular access control, video security, alarms in the event of unauthorized access and fire protection. In order to optimally protect critical assets, zones with a higher protection category can only be accessed if previous rooms with a lower protection category have been accessed (shell principle).

— Services

We provide services in all phases of the development and operation of buildings and systems. Our 360° services enable efficiency benefits and innovation. We ensure optimal operation as early as the planning stage.

— Effective perimeter protection

Intelligent perimeter protection is the most effective measure in preventing unauthorized access, sabotage, vandalism and theft. With our end-to-end solution you achieve three core objectives:

— Reliably detect hazards

Despite difficult environmental conditions such as vegetation, weather or darkness the optimal perimeter protection solution detects safety-relevant events.

— Ensuring future viability

With services that keep hardware and software up to date we can ensure the best possible security for the future.

— Increase operating efficiency

An intelligently networked security system helps avoid false alarms and automates processes as much as possible. Analysis Dashboards support cross-site optimization.

— Perfect interaction: the control center reacts to events within a multi-level safety system

Conventional mechanical safeguards such as fences or walls can be overcome. Early detection of security-relevant events in the outdoor area averts threats and gains valuable reaction time for intervention measures. The control center responds to events in a multi-level system. Messages from different zones are linked logically and visualized in the hazard management system.

— Event detection at the fence

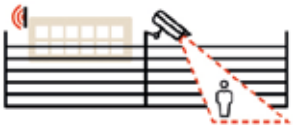
Intelligent fence sensor technology detects safety-related activities such as attempts to climb over, cutting and pushing, while avoiding false alarms caused by wind, for example. In cases where there is a site without a physical barrier, infrared technology and intelligent video analysis form a virtual perimeter.

Mechanical systems, position and seismic sensor, laser detector and IP video technology

— Perpetrator approach for initial deterrence

An automated, event-driven approach via recorded audio clips deters offenders.

IP audio systems



— Reliable detection of intruders

Thermal cameras along the perimeter and laser detectors (LiDAR) detect people entering the premises, even in absolute darkness. Intelligent analysis functions with object classification avoid false alarms.

Thermal imaging technology, laser detectors (LiDAR) and IP video technology

— Targeted offender tracking

High-performance PTZ cameras automatically track the perpetrator. The emergency call and service control center knows the position of the perpetrator at all times and can control intervention personnel in a targeted manner.

IP video technology / PTZ cameras, PSIM platform

— Remote management 24/7 and video search

After the visualization of events in the hazard management system, the security control center verifies the alarm on the basis of live images from IP video cameras and takes over the targeted control of intervention personnel. By means of cross-camera video search including facial recognition as well as analysis of object movements and behavioral trends, suspicious persons and objects can be quickly detected and localized.

Analysis software, PSIM platform

— Automated access process with customized functionality

Access control is an essential for the physical protection of critical infrastructures. The challenge here lies not only in reliable authentication and separation, but also in the digitalization and user-centered design of the entire process.

Accordingly, we develop end-to-end access solutions along user journeys of relevant personas. Our use cases range from digital visitor management with identity verification and the control of people and material flow in complex areas, such as loading bays and carpark management.

— Use Case Overview

Access control with anti-passback and zone change management

Entry and exit control

Parking Facility Management

Digital Access Management with Identity Verification

People and material flow control

Personal control by microwave technology

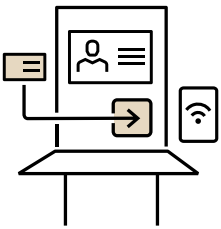
Elevator control system

Escape route safety and security

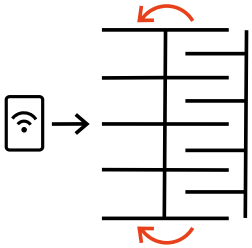
— Example of an integrated access solution for data centers

The end-to-end access solutions along the user journey of an external technician in the data center automates and accelerates the check-in process with identity verification, security briefing and badge generation, taking into account the highest security standards. At the same time, documented and monitored authentification takes place at every zone transition from campus access to IT rack opening. Individual entry into rooms with the highest protection categories is supported by sensors. Depending on the protection goal, we integrate security screening based on microwave technology with artificial intelligence.

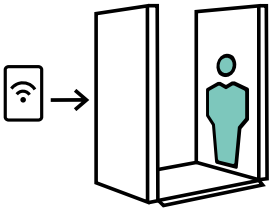
Access Management with Identity Verification



Controlled access



Separation and personal control



Security
Risk score

— 1
essentry-Kiosk
ID-Authentication,
Biometric Face
Matching

Reception

— 2
RFID-Card reader
Turnstiles

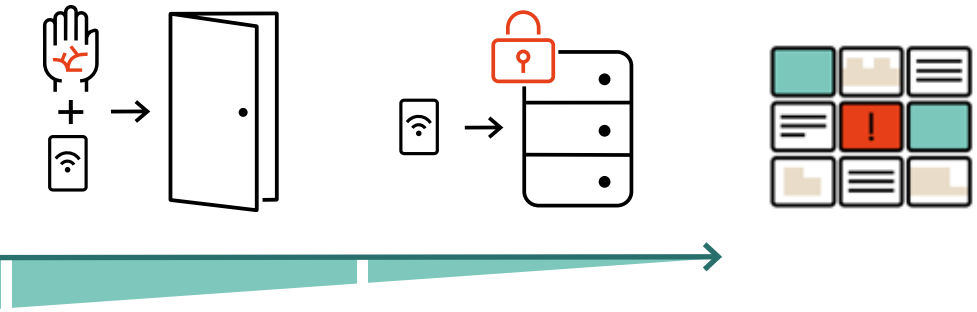
Secured campus

— 3
Card reader
Person airlock
Room airlock with
Bodyscanner

Building

Controlled access only after successful screening

Holistic overview



— 4
RFID Card reader
Palm vein scanner
ATG sensor technology
Door monitoring

IT Area

— 5
Electronic rack lock
with RFID reader
Door monitoring

Rack

— 6
24/7 Monitoring
and AI-supported
Hazard Management

Alarm Monitoring Center

— Digital Visitor Management for Critical Infrastructures

We digitize access management for critical infrastructures in a secure, simple and user-centered way. We seamlessly integrate the access management system from essentry into your existing access control system, enabling an automated check-in process with identity verification, security briefing and badge generation. In this way, we reduce the process time to less than one minute while increasing the level of security.

— Identity verification

We verify visitor identity reliably and securely – and at border control level, thereby checking the authenticity of more than 7,500 identity documents from 196 countries.

Artificial intelligence is used to match the image on the ID document with a 3D portrait taken on-site.

— Automation of check-in process

Via the essentry platform, a large number of preparations can already be done digitally and before the visit, e.g., signing NDAs, safety briefings or health briefings. The check-in process takes less than a minute.

After successful identity verification, the guest automatically receives an RFID card with individual access authorization.

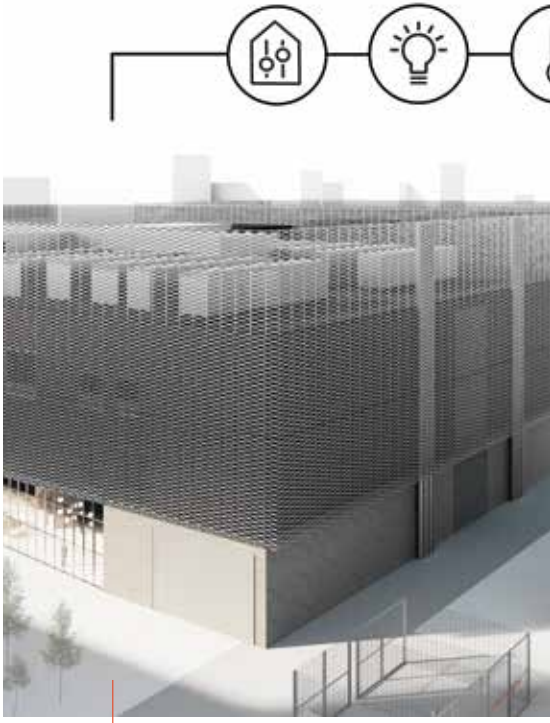
— Customization of check-in

The essentry system is highly flexible and can be adapted to individual company needs.

To simplify and accelerate the check-in process for returning visitors, for example, you can create „Trusted IDs" for permanent use.

— 24/7 Monitoring and AI-supported Hazard Management

We integrate all security systems and IoT sensors in a unified management platform. In this way, we create a complete security overview, even across different locations.



Integration

— Security systems (FAS, IAS, Video, ACS etc.)
— IoT-sensors (room teperature, VOC, position, presence etc.)
— Building and communications technology

Control

— Dynamic proces instructions
— Automated operations
— Switching operations (e.g., switching systems off and on, remote door opening system)

Transparency

— Intelligent visualization of events in campus and building maps
— Analysis & dashboards

Live-images

— Event video images

We use decentralized intelligence to detect security-related events and avoid false alarms. This helps security personnel focus on verified alarms, which are visualized in site and floor plans in the hazard management system.

Our certified alarm receiving center (DIN EN 50518) and our service control center network (VdS 3138 and 3138–2) handle the operation of the integrated security systems as well as the alarm management 24/7 (DIN EN 9001–2015) or in a defined time window for redundancy, if you have your own staff. The control of the intervention personnel and resources is carried out with the support of the hazard management system based on defined workflows.

VdS

AES (DIN EN 50518)
NSL (VdS 3138 und 3138–2)

Get a complete security picture at any time. Dashboards help to make decisions and continuously optimize systems and processes.

— Strong Partners

We integrate only cutting-edge technologies from leading, innovative companies with whom we have a long-standing partnership. From a range of security and IoT products, we make the best selection for our customers and develop a holistic 360° solution that, thanks to interoperability, can be fit perfectly into the existing systems.

— We integrate cutting-edge technologies from leading, innovative companies

— We integrate cutting-edge technologies from leading, innovative companies

— Our System
Your Advantage

We enable a holistic security situation. We ensure the early detection of hazards and transform sensor data into automated actions for efficient security management.

— Highest security

Through multi-stage systems, intelligent analysis functions, and alarm management with 24/7 service availability, threats are reliably detected and averted.

— More transparency

By integrating various systems and central monitoring, we create a holistic security environment and help the security team make better decisions.

— Reliable quality

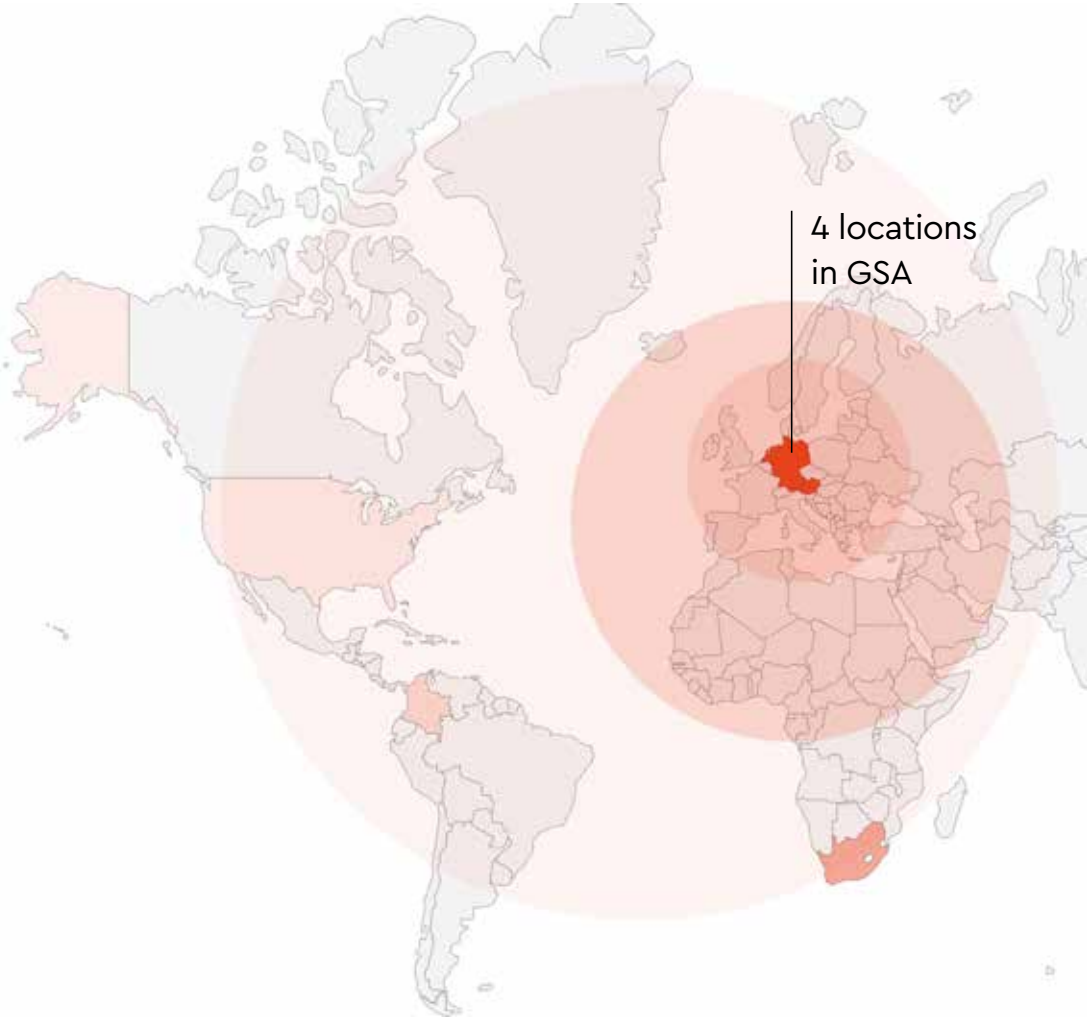
You receive all our services from a single source. At the same time, we ensure reliable implementation through the quality work of our technical team.

— Better user experience

By designing end-to-end security solutions along the user journeys of relevant personas and digitizing processes, we enhance the user experience and enable you to seamlessly integrate security into everyday life.

— Higher cost efficiency

Through standardization, automation, and a service concept, which covers all services from planning and implementation to 24/7 monitoring and hazard management, we achieve the greatest possible cost-effectiveness.



From Berlin | Frankfurt | Munich | Vienna all over the world

— Our experience

We combine industry experience with system integration competence and the ability to innovate.

300+

— Enterprise-level systems and multisite applications

Experts for holistic security solutions, digitalization and automation

— Certified Systems

Expert-level certification of leading technologies
ISO 9001:2015, DIN 14675, VdS 3403, VdS 3138, DIN EN 50518

20+

Years of experience

with the implementation of integrated security solutions for CRITIS

Your route to a holistic security solution

Our experts for security technology and Building IoT look forward to helping you design, implement and operate your integrated solution.

— Contact us!

e-shelter security
Eschborner Landstraße 100
60489 Frankfurt am Main
+49 69 247 430 – 000

sales@e-shelter.io
e-shelter.io

e-shelter security
Eschborner Landstraße 100
60489 Frankfurt am Main
+49 69 247 430 – 000
info@e-shelter.io
e-shelter.io

© 2024 e-shelter security GmbH
Alle Rechte vorbehalten. Die Informationen in dieser Broschüre enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsabschluss ausdrücklich vereinbart werden. Liefermöglichkeiten und technische Änderungen vorbehalten.